DEMP Specification

DEMP-SPEC 0.5.0

13 January 2026

Revision history: `https://demp.ch/spec/CHANGELOG.md`

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119.

The Markdown (MD) document is the canonical source for this version of the specification. In case of any inconsistency with other representations, the Markdown document SHALL prevail.

Table of Contents

1 Scope

The **Decentralized Emergency Management Protocol (DEMP)** ensures secure, interoperable and decentralized communication between Safety Information Systems (SIS), whether operating as standalone instances or within a federated network. It facilitates real-time data exchange across safety zones, entities, and devices, enabling seamless coordination and an effective, community-driven and digitally enhanced response during emergencies.

The **Decentralized Emergency Management Protocol Specification (DEMP-SPEC)** defines a technical standard that outlines a framework and guidelines for implementing and interacting with decentralized emergency management systems built on DEMP.

The primary goal of this specification is to provide comprehensive documentation for developers and integrators, enabling them to create or integrate DEMP-based systems and applications. It describes the components, rules, and data structures necessary for the successful deployment of safety information systems in various environments.

It is important to note that this specification does not address the organizational or operational implementation of Safety Information Systems (SIS), nor does it cover the detailed design of software or hardware devices.

2 Audience

The specification is intended for a variety of stakeholders involved in the development, integration, and operation of decentralized emergency management systems. The primary audience includes:

- **System Architects and Developers**: Those designing and developing DEMP-compliant software.
- **Integrators**: Professionals responsible for integrating DEMP-compliant solutions.
- **Device Manufacturers**: Organizations that produce DEMP-compliant devices.
- **Security and Safety Specialists**: Professionals involved in emergency management.
- **Cybersecurity Specialists**: Professionals involved information security and cyber risk management.
- **Lawyers**: Legal professionals ensuring that DEMP complies with relevant laws and regulations.
- **Policy Makers and Regulators**: Authorities responsible for regulating emergency management systems.
- **Volunteers**: Individuals and communities actively promoting the adoption and implementation of DEMP.

3 Versioning

The document follows **Semantic Versioning (SemVer) 2.0.0** to manage its releases and updates. This approach ensures that developers and integrators can understand the impact of each version based on the changes made in the specification.

4 Contributors

- **Jean-Pierre Grossglauser**: Lead Author, System Architect

5 Architecture

5.1 Network

A **DEMP Network MUST** form the backbone for communication between multiple Safety Information Systems (SIS).

5.1.1 Decentralization

There **MUST** be no central authority managing the DEMP Network operations.

5.1.2 Interoperability

A DEMP Network **MUST** support interoperability between different Safety Information System (SIS) implementations, ensuring that they can securely communicate with each other, regardless of their underlying hardware, software or geographical location.

5.1.3 Communication

A DEMP Network **SHOULD** rely on the Internet Protocol (IP) for communication and the Domain Name System (DNS) for naming and addressing purposes.

5.1.4 Scalability

A **DEMP Network MUST** be designed to scale dynamically, allowing Safety Information Systems (SIS) to be added to or removed from the network without disrupting ongoing operations or compromising availability.

5.1.5 Scope

Wide Area Network (WAN) A **DEMP Network SHOULD** be able to operate across Wide Area Networks (WAN), including the public Internet, to enable communication and federation between geographically distributed Safety Information Systems (SIS).

Local Area Network (LAN) A **DEMP Network SHOULD** be able to operate within a Local Area Network (LAN), enabling Safety Information Systems (SIS) to function autonomously in isolated, offline or network-restricted environments.

Virtual Private Network (VPN) A **DEMP Network SHOULD** support operation over Virtual Private Networks (VPN), enabling secure and controlled interconnection between geographically or administratively separate Safety Information Systems (SIS).

Ad Hoc Network A **DEMP Network MAY** support operation within a local mesh or peer-to-peer (P2P) ad hoc network that enables offline or short-range secure data exchange.

5.1.6 Discovery

Directory A **DEMP Network MAY** provide a directory to facilitate discovery of participating Safety Information Systems (SIS).
Any such directory **MUST** maintain an up-to-date registry of participating Safety Information Systems (SIS).

Participation Participation in any discovery mechanism **MUST** be voluntary.
A Safety Information System (SIS) **MUST** be able to opt in to or opt out of a Network Directory without affecting its ability to operate within the DEMP Network.

5.2 Safety Information System (SIS)

A **Safety Information System (SIS) MUST** monitor, manage, process and exchange safety-related data for Entities and between Safety Information Systems (SIS), either as a standalone server instance or as a participant in a Federation.

5.2.1 Data Exchange

A Safety Information System (SIS) **SHOULD** ensure reliable communication and information exchange with Entities and other Safety Information Systems (SIS), taking into account latency, bandwidth usage and availability constraints.

5.2.2 Data Processing

A Safety Information System (SIS) **MUST** process DEMP data in accordance with applicable privacy requirements.

5.2.3 Data Storage

A Safety Information System (SIS) **MAY** store DEMP data required for operation, recovery, and auditability.

5.2.4 Security

A Safety Information System (SIS) **MUST** protect data exchange, data processing, and data storage against unauthorized access and tampering through appropriate technical and organizational measures.

5.2.5 Autonomy

A Safety Information System (SIS) **MUST** be capable of operating autonomously within its defined scope, without requiring continuous connectivity to other Safety Information Systems or external services.

5.2.6 Deployment

A Safety Information System (SIS) **SHOULD** be deployed in a stable, managed and production-grade environment appropriate for continuous operation, scalability and appropriate levels of availability.

5.2.7 Hub

A Safety Information System (SIS) **MUST** be accessible by Entities through an access point called a **Hub**.

Interface A **Hub SHOULD** be a secure HTTP service providing web-based access to administrative information and interaction features for Entities.

Access Control Access to the **Hub MUST** be either public or private (network-restricted). It **MAY** also be subject to authentication.

5.3 Safety Zone

A **Safety Zone** (Zone) **MUST** be a defined physical or virtual area that is monitored for safety events and emergency management purposes.

5.3.1 Physical Zones

A **Physical Zone MUST** be defined by accurate **spatial references**.

Mobility A **Physical Zone MAY** be either *static* or *dynamic*, depending on whether its **spatial references** remain constant over time.

5.3.2 Virtual Zones

A **Virtual Zone MUST** be based on logical boundaries without spatial reference requirements.

5.3.3 Temporality

A **Safety Zone MAY** be defined temporarily for particular time-based events.

Time Boundaries Such zones **MUST** have explicitly defined start and end times specified in Coordinated Universal Time (UTC).

5.4 Entity

An **Entity MUST** represent a participant interacting with a Safety Information System (SIS) and **MUST** be assigned exactly one Entity role.

5.4.1 Roles

An **Entity MUST** be assigned exactly one of the following roles, which define the nature of the participant interacting with a Safety Information System (SIS):

- **Individual**: An Entity with this role **MUST** represent a single human person acting in an individual capacity.
- **Organization**: An Entity with this role **MUST** represent a structured group, institution or legal organization acting as a collective participant.
- **Autonomous Agent**: An Entity with this role **MUST** represent a software-based agent capable of operating autonomously and interacting with the SIS without direct human intervention.

A Safety Information System (SIS) **MAY** define additional Entity roles for internal or domain-specific use; in such cases, the SIS **MUST** ensure interoperability.

5.4.2 Identification

An **Entity MUST** be uniquely identifiable within a Safety Information System (SIS).

5.4.3 Authentication

An **Entity MUST** authenticate to the Safety Information System (SIS) before any interaction or action can be performed.

Individuals Entities with the **Individual** role **MUST** use multi-factor authentication, where at least one of the factors is biometric.

Organizations Entities with the **Organization** role **MUST** use cryptographic authentication.

Autonomous Agents Entities with the **Autonomous Agent** role **MUST** use cryptographic authentication.

5.5 Device

Devices **MUST** be able to exchange data with a Safety Information System (SIS) on behalf of an Entity.

5.5.1 Device Types

A Device **MUST** be classified as either a **Software Device** or a **Hardware Device**. This classification **SHOULD** be taken into account by the Safety Information System (SIS) to ensure appropriate interaction and handling.

5.5.2 Device Modes

A Device **MUST** operate in either **Active** or **Passive** mode. The selected mode defines how the Device may interact with the Safety Information System (SIS).

Active Devices An **Active Device MUST** be capable of both sending data to and receiving data from the Safety Information System (SIS).

Passive Devices A **Passive Device MUST** be capable of sharing data with the Safety Information System (SIS), but **MUST NOT** initiate communication.

5.6 Alert

An **Alert MUST** represent a safety, security or emergency situation managed by a Safety Information System (SIS).

5.6.1 Alert Status

Each Alert **MUST** have exactly one status that reflects its current state within the Safety Information System (SIS).

At least the following alert statuses **MUST** be defined, supported and interpreted as follows:

- **Reported**: An Alert with this status **MUST** indicate that the alert has been triggered by the Safety Information System (SIS).
- **Responding**: An Alert with this status **MUST** indicate that response, coordination or mitigation actions are currently being performed.
- **Resolved**: An Alert with this status **MUST** indicate that the situation has been addressed and that no further response action is required.
- **Rejected**: An Alert with this status **MUST** indicate that the alert has been dismissed and **MUST NOT** require further action.

A Safety Information System (SIS) **MAY** define additional Alert status for internal or domain-specific use; in such cases, the SIS **MUST** ensure interoperability.

5.6.2 Alert Level

Alert level **MUST** indicate the escalation tier of an alert and define the expected response and handling obligations.

At least the following alert levels **MUST** be defined and interpreted as follows:

- **Test**: Alerts of this level **MUST** be used exclusively for testing or training purposes and **MUST NOT** represent real situations.
- **Information**: Alerts of this level **MUST** be intended to convey general information and **MUST NOT** require action or confirmation of reception.
- **Warning**: Alerts of this level **MUST** represent potential safety issues and **MUST** require confirmation of reception.
- **Emergency**: Alerts of this level **MUST** represent situations requiring immediate intervention.

A Safety Information System (SIS) **MAY** define additional Alert levels for internal or domain-specific use; in such cases, the SIS **MUST** ensure interoperability.

5.6.3 Zone Alert

A **Zone Alert MUST** be generated for situations that could affect a specific physical or virtual Safety Zone within a SIS.

5.6.4 System Alert

A **System Alert MUST** be generated for situations that could affect all Safety Zones within a SIS.

5.6.5 Federated Alert

A **Federated Alert MUST** be generated for situations that could impact multiple Safety Information Systems (SIS) participating in a Federation.

5.6.6 Open Alert

An **Open Alert MUST** be generated for situations requiring widespread propagation across a DEMP Network.

Propagation An **Open Alert MUST** be forwarded to every Federation a SIS is a member of.

Each Federated SIS **SHOULD** propagate the alert according to the Federation's Open Alert Policy (OAP).

Third-party SIS **MAY** further propagate the alert beyond their Federations according to their respective policies.

5.7 Federation

A **Federation MUST** be a group of Safety Information Systems (SIS) that formally collaborate to share information and coordinate safety and emergency management.

5.7.1 Structure

Federations **MAY** adopt a **Hierarchical Federation** structure.

A **Hierarchical Federation MUST** be composed of multiple federation levels, where a Safety Information System (SIS) may federate with other SIS operating at different scales.

This hierarchy **MAY** reflect differences in operational scope, geographical coverage, responsibility, or jurisdiction.

A **Hierarchical Federation MUST NOT** inherently impose centralized authority or mandatory decision-making control across federation levels. Any authority or responsibility exercised across levels **MUST** be explicitly defined and agreed upon by the participating federation members.

5.7.2 Alert Management Agreement (AMA)

A **Federation SHOULD** define an **Alert Management Agreement (AMA)** describing how Federated Alerts are triggered, escalated and handled across member Safety Information Systems (SIS).

5.7.3 Consensus Decision-Making Agreement (CDMA)

A Federation **SHOULD** establish a Consensus Decision-Making Agreement (CDMA) defining voting mechanisms and any extended decision-making privileges within the authorization model, where applicable.

5.7.4 Conflict Resolution Agreement (CRA)

A **Federation SHOULD** define a **Conflict Resolution Agreement (CRA)** describing how conflicts between members are resolved.

5.7.5 Open Alert Policy (OAP)

A **Federation SHOULD** establish a common **Open Alert Policy (OAP)** defining the conditions under which members handle **Open Alerts**.

5.8 Consensus Decision-Making (CDM)

A Safety Information System (SIS) or Federation **MAY** implement a Consensus Decision-Making process to coordinate significant decisions involving multiple participating entities.

5.8.1 Time-Bound Polling

The polling mechanism **MAY** be time-bound to ensure prompt decision-making.

5.8.2 Tie-Breaking

Repeated Poll A Safety Information System (SIS) **MAY** repeat a poll provided that the alert severity is below a defined critical threshold and sufficient time remains within the applicable decision window.

Deterministic Fail-Safe Resolution If a repeated poll is not feasible due to alert level, time constraints or any other reason, the Safety Information System (SIS) **MUST** apply a deterministic fallback procedure.

6 Certification

Certification **MUST** establish *verifiable trust claims* that can be independently validated through the Chain of Trust.

6.1 Independent Certification Authority (ICA)

An **Independent Certification Authority (ICA) MUST** be an independent organization responsible for evaluating and certifying subjects defined by this specification according to the applicable certification requirements and framework.

An ICA:

- **MUST** be organizationally and operationally independent from the subject it certifies
- **MUST** apply evaluation criteria that are publicly available
- **MUST** apply evaluation criteria consistently to all subjects it certifies
- **MUST** be clearly identifiable and accountable
- **MUST** support certification lifecycle management, including issuance, expiry, suspension, and revocation

6.1.1 Oversight

Independent Certification Authorities (ICA) **MAY** perform peer oversight of other ICAs to assess compliance and adherence to recognized best practices.

6.2 Certification Framework

Any certification issued under the Certification Framework:

- **MUST** be issued by an Independent Certification Authority (ICA)
- **MUST** be unambiguously attributable to a specific ICA
- **MUST** be time-bounded, with an explicit validity period
- **MUST** support suspension and revocation
- **MUST** be cryptographically verifiable

Certification **MUST** result in a verifiable certification assertion that can be independently validated through the Chain of Trust.

6.3 Certified Safety Information System

A Safety Information System (SIS) **MUST** be considered a **Certified Safety Information System** when it holds a valid certification.

6.4 Certified Entity

An Entity **MUST** be considered a **Certified Entity** when it holds a valid certification.

7 Authorization

A Safety Information System (SIS) **MUST** implement a privileges-based authorization model to control actions performed by Entities.

7.1 Extended Privileges

Extended privileges **MUST** represent authorization grants that exceed the default operational or decision-making capabilities of an Entity.

Extended privileges:

- **MUST** be granted explicitly through the privileges-based authorization model
- **MUST** be limited in scope and purpose
- **MUST** be time-bounded
- **MUST** be applicable only to an Entity with a valid Certification

Extended privileges **MAY** be defined at the Safety Information System (SIS) or Federation level.

8 Chain of Trust

The Chain of Trust **MUST** define the technical and procedural mechanisms by which a Safety Information System (SIS) verifies trust, enforces trust-based decisions and records trust-relevant events.

8.1 Trust Assertions

The Chain of Trust **MUST** operate on **trust assertions**, defined as cryptographically verifiable claims derived from certifications issued under the Certification Framework.

8.2 Auditability

Trust-related events **MUST** be auditable.

Auditability **MUST** allow independent verification that trust-related lifecycle events occurred, were not altered, removed or suppressed.

8.2.1 Pseudonymity

Audit records **MUST** be pseudonymous by design.

8.2.2 Registry

To support immutability and non-repudiation, trust-related lifecycle events **MUST** be recorded in an append-only audit registry.